UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/713,560	11/14/2003	Richard Bussiere	ENI-037	8242

35557 7590 06/12/2006

CHRIS A. CASEIRO
VERRILL DANA, LLP
ONE PORTLAND SQUARE
PORTLAND, ME 04112-0586

EXAMINER	
SZYMANSKI, THOMAS M	
ART UNIT	**PAPER NUMBER**
2134	

DATE MAILED: 06/12/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/713,560	BUSSIERE ET AL.	
	Examiner	Art Unit	
	Thomas Szymanski	2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *17 November 2003*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-27* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-27* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *17 November 2003* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *1/3/05*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-27 have been examined.

Specification

2. The lengthy specification has not been checked to the extent necessary to determine the presence of all possible minor errors. Applicant's cooperation is requested in correcting any errors of which applicant may become aware in the specification.

Claim Rejections - 35 USC § 102

3. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

4. Claims 1-27 are rejected under 35 U.S.C. 102(b) as being anticipated by Huff et al International Publication No. WO 99/57625 (hereinafter "Huff").

5. Regarding Claim 1: A method of responding to the detection of an intrusion on a network system that provides network services, the network system including one or more attached functions and one or more network infrastructures, the method comprising the steps of: a. monitoring the network system for intrusions (Abstract, Fig 1, 3, pg 5 lines 2-5)

b. upon detection of an intrusion, identifying one or more sources of the intrusion (pg 5 lines 6-9, 12-16, pg 12 line 29 – pg 13 line 3, pg 18 line 27 – pg 19 line 13, pg 20 lines

3-5, pg 21 lines 10-13) Identifying the source of the intrusion occurs two fold within the system of Huff by not only detecting the device on the local network where the issue arise but by tracing the remote location as well.

c. identifying one or more enforcement devices of the network system associated with the one or more identified sources (Fig 3-4, pg 4 line 11 – pg 5 line 30, pg 14 line 3 – pg 15 line 10, pg 18 lines 16-26) As depicted by Huff agents associated with intrusion events are identified and send information back to the central server.

d. configuring the identified one or more enforcement devices with one or more policy changes responsive to the detected intrusion (Fig 3-4, pg 4 line 11 – pg 7 line 11, pg 13 lines 10-12, pg 14 lines 6-12, pg 15 lines 3-11, pg 17 lines 14-25, pg 18 lines 1-pg 19 line 25) In response to intrusion detections the system takes actions by changing current monitoring policies or access policies.

6. Regarding Claim 2: The method as claimed in Claim 1 wherein the step of identifying the one or more sources of the intrusions includes the step of identifying a physical address and/or a logical address of each of the one or more identified sources (pg 8 lines 24-30, pg 11 lines 5-23, pg 12 line 30 – pg 13 line 2, 23-27, pg 18 line 27 – pg 19 line 13, pg 20 lines 3-5, pg 21 lines 10-13)

7. Regarding Claim 3: The method as claimed in Claim 2 wherein the physical address information is a MAC address and/or the logical address information is an IP address (pg 8 lines 24-30, pg 11 lines 5-23, pg 12 line 30 – pg 13 line 2, 23-27, pg 18 line 27 – pg 19 line 13, pg 20 lines 3-5, pg 21 lines 10-13) As provided by Huff the use of ethernet type networks dictates that for address resolution purposes, which is an

inherent functionality of such a network, addresses are stripped from packets which contain both MAC and IP type addresses. Furthermore, as stated since all devices are addressable on the network and the implementation of any such protocol as TCP/IP dictates resolution of such devices occurs via a MAC address associated to an IP address.

8. Regarding Claim 4: The method as claimed in Claim 1 wherein the step of monitoring the network for intrusions is performed by an intrusion detection function (pg 4 line 11 – pg 7 line 11, pg 12 lines 15-21, pg 18 lines 1-10, 27-30) Monitoring the network occurs in a distributed manner with all indications sent back to a central server for analysis.

9. Regarding Claim 5: The method as claimed in Claim 4 wherein the intrusion detection function is a centralized function (Fig 3, pg 4 line 11 – pg 7 line 11, pg 11 lines 25-30) the intrusion detection function is centralized by the security server that controls actions taken by the distributed agents.

10. Regarding Claim 6: The method as claimed in Claim 4 wherein the intrusion detection function is a distributed function (Fig 3, pg 4 line 11 – pg 7 line 11, pg 17 lines 8-15, pg 20 lines 15-16)

11. Regarding Claim 7: The method as claimed in Claim 4 wherein the intrusion detection function is an intrusion detection system (pg 4 line 11 – pg 7 line 11) The functions are correlated together through the central server into a system.

12. Regarding Claim 8: The method as claimed in Claim 1 wherein the step of identifying the one or more enforcement devices associated with the one or more

identified sources includes the step of determining the physical address, logical address, or both for each of the identified one or more enforcement devices (pg 8 lines 24-30, pg 11 lines 5-23, pg 12 line 30 – pg 13 line 2, 23-27, pg 18 line 27 – pg 19 line 13, pg 20 lines 3-5, pg 21 lines 10-13) Resolution of addresses in order to send messages and communicate actions must take place via such a path.

13. Regarding Claim 9: The method as claimed in Claim 1 further comprising the step of verifying the identification of the identified one or more sources (pg 5 lines 6-9, 12-16, pg 12 line 29 – pg 13 line 3, pg 18 line 27 – pg 19 line 13, pg 20 lines 3-5, pg 21 lines 10-13) Huff states that agents serve to verify the identity of the source through the steps of tracing.

14. Regarding Claim 10: The method as claimed in Claim 1 wherein the step of configuring the identified one or more enforcement devices with one or more policy changes responsive to the detected intrusion includes the step of configuring the identified one or more enforcement devices to perform one or more functions selected from the group consisting of: blocking complete access to the network services by the identified one or more sources, blocking access by identified logical addresses only, blocking access by an identified access protocol only, limiting bandwidth, limiting exchanges to or from the identified one or more enforcement devices, to or from one or more other network infrastructure devices, or to or from any of the attached functions not identified as an intrusion source (pg 4 line 11 – pg 7 line 11, pg 18 line 1 –pg 19 line 25, pg 22 lines 3-20) The intruder is either disabled, which consists of disabling that

connection, or is misdirected toward information that cannot be harmed in order to collect further information about the intruder.

and directing all signals exchanged by the identified one or more sources to a honey-pot, a second intrusion detection function, a monitoring device, or a simulation device (pg 18 line 1 –pg 19 line 25, pg 20 lines 2-8, pg 20 lines 27- pg 21 line 1, pg 21 lines 10-30, pg 22 lines 3-20) The intrusion system directs all information back to the central server which stores information within a database.

15. Regarding Claim 11: The method as claimed in Claim 1 wherein the step of configuring the identified one or more enforcement devices with one or more policy changes responsive to the detected intrusion includes the step of configuring the identified one or more enforcement devices to permit connectivity of the identified one or more sources while dampening the level of activity associated with the identified one or more sources to minimize network harm while permitting analysis and auditing of the identified one or more sources and the gathering of forensic evidence (pg 17 line 18 – pg 19 line 14, pg 21 line 6 – pg 22 line 19) as recited the intruder is misdirected toward data to decrease any possible harm to the network in order to collect data about the attacker.

16. Regarding Claim 12: The method as claimed in Claim 1 wherein the step of configuring the identified one or more enforcement devices with one or more policy changes includes the steps of first configuring a first set of one or more enforcement devices with a first set of one or more policy changes, monitoring the network system for intrusions and, upon detection of one or more intrusions related to the intrusions

causing the first one or more policy changes, configuring a second set of one or more enforcement devices with a second set of one or more policy changes (pg 17 line 18 – pg 19 line 14, pg 21 line 6 – pg 22 line 19) Audit levels may be changed as well as having the attacker misdirected for further examination. Upon detection of further activity from the increase in auditing further actions can be taken by the system to have the attacker disabled or misdirected.

17. Regarding Claim 13: The method as claimed in Claim 12 wherein one or more of the one or more enforcement devices of the second set are enforcement devices of the first set (Fig 3, pg 15 lines 3-11, pg 17 lines 8-22, pg 18 lines 1-12, pg 19 lines 1-14) The system has agents on nodes that monitor for intrusions, when an intrusion or suspicious activity is detected the audit level can be increased and upon further inspection if such activity is determined to be inappropriate further action can be taken by the agent.

18. Regarding Claim 14: The method as claimed in Claim 1 wherein the identified one or more enforcement devices are selected from the group consisting of network entry devices and centralized switching devices (pg 8 lines 24-30, pg 9 lines 12-15, pg 13 lines 24-26) Such devices as firewalls are embodied as network computing devices and thus are anticipated by the present invention. Additionally, Huff states that any node on the network is foreseeable as implementing the agents (enforcement devices), as such anticipating switches.

19. Regarding Claim 15: The method as claimed in Claim 1 wherein the one or more policy changes are configured on one or more ports of one or more of the identified one

or more enforcement devices (pg 14 lines 26—pg 15 line 2) Huff provides for configuring agents through associated ports.

20. Regarding Claim 16: a directory service function for receiving address information for attached functions and devices of the network infrastructure; a policy manager function for configuring devices of the network infrastructure with policies (Fig 4, pg 18 lines 15-26) Huff provides a directory of all monitored devices and there associated enforcement mechanisms. Further, there are means associated with the directory for changing policies and also within the automatic response for implementing and changing policies.

21. Claims 17-27 are further embodiments of the above rejected claims and as such are rejected on the same basis.

Conclusion

22. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. Applicant is reminded that in amending in response to a rejection of claims, the patentable novelty must be clearly shown in view of the state of art disclosed by the references cited and the objections made. Applicant must show how the amendments avoid such references and objections. See 37 CFR 1.111(c).

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Thomas Szymanski whose telephone number is 571-272-8574. The examiner can normally be reached on M-F 8-4:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Jacques Louis-Jacques can be reached on 571-272-6962. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

TMS